Page 2053 - 2063

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

A Comparative Analysis of India's Digital Personal Data Protection Act, 2023 and the EU General Data Protection Regulation

OJASHWI SIDHARTH*

ABSTRACT

The rapid expansion of digital technologies and data-driven economies has intensified concerns regarding privacy, surveillance, and the misuse of personal information. In response, nations across the globe have enacted comprehensive data protection laws to regulate the collection, processing, storage, and transfer of personal data. India introduced the Digital Personal Data Protection Act, 2023 (DPDP Act) as its first comprehensive legislation dedicated exclusively to personal data protection, while the European Union's General Data Protection Regulation (GDPR), implemented in 2018, is regarded as one of the world's most stringent and influential privacy frameworks. This paper undertakes a comparative analysis of the DPDP Act, 2023 and the GDPR by examining their objectives, scope, principles, the rights of individuals, the obligations of data fiduciaries and controllers, cross-border data-transfer mechanisms, enforcement structures, and penalties. The paper further evaluates the extent to which the Indian legislation aligns with international privacy standards and identifies significant divergences between the two frameworks. While the GDPR adopts a rights-centric and stringent regulatory model emphasising accountability and individual autonomy, the DPDP Act reflects a comparatively flexible and State-oriented approach that balances privacy with governance and economic considerations. The analysis highlights the strengths and limitations of both frameworks and discusses the implications for multinational corporations, digital governance, and the future of privacy protection in India. This paper concludes that, although the DPDP Act marks a significant milestone in India's digital regulatory landscape, further reforms and institutional safeguards may be necessary to achieve parity with the global standards established by the GDPR.

I. INTRODUCTION

The digital age has transformed personal data into one of the most valuable resources in the global economy. Governments, corporations, and digital platforms routinely collect and process

* Author is an LL.M. student at Bharati Vidyapeeth University, New Law College, Pune, Maharashtra, India.

 [ISSN 2581-5369]

vast amounts of personal information for commercial, administrative, and technological purposes. While such practices facilitate innovation and economic growth, they also create serious concerns relating to privacy violations, data breaches, identity theft, unauthorised surveillance, and the misuse of sensitive personal information. Consequently, data protection has emerged as a crucial aspect of contemporary governance and human-rights discourse.

The recognition of privacy as a fundamental right by the Supreme Court of India in *Justice K.S. Puttaswamy v. Union of India*[1] laid the constitutional foundation for comprehensive data protection legislation in India. Following years of legislative deliberation, India enacted the Digital Personal Data Protection Act, 2023[2] to regulate the processing of digital personal data and to establish obligations for entities handling such information. The legislation seeks to create a framework that balances the rights of individuals with the legitimate needs of businesses and the State.

In contrast, the European Union introduced the General Data Protection Regulation in 2018[3] with the objective of harmonising data protection laws across member states and strengthening individual control over personal information. The GDPR is widely regarded as the global benchmark for privacy regulation owing to its detailed provisions, stringent compliance requirements, and extraterritorial application.

Although both instruments aim to safeguard personal data, their approaches differ significantly in terms of structure, enforcement, and regulatory philosophy. This paper comparatively examines the DPDP Act, 2023 and the GDPR to understand their similarities, differences, and practical implications in the evolving digital ecosystem.

II. EVOLUTION OF DATA PROTECTION LAWS

Data protection laws developed in response to increasing concerns about computerised data processing and the growing influence of digital technologies. European countries were among the first to establish privacy regulation during the late twentieth century, and the European Union gradually consolidated these standards through the Data Protection Directive of 1995,[4] which later evolved into the GDPR. The GDPR represented a major shift from fragmented national laws toward a unified and enforceable framework emphasising transparency,

[1] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).
[2] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[3] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[4] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 (Data Protection Directive), 1995 O.J. (L 281) 31.

 [ISSN 2581-5369]

accountability, and individual rights. Its enactment significantly influenced global data governance and encouraged many countries to modernise their privacy laws.

India's journey toward comprehensive data protection legislation evolved more gradually. Initially, privacy protections were scattered across the Information Technology Act, 2000 and related rules.[5] However, the absence of a dedicated framework became increasingly problematic in light of expanding digital services and frequent data breaches. The landmark *Puttaswamy* judgment in 2017 recognised privacy as an intrinsic part of Article 21 of the Constitution, thereby necessitating legislative intervention. Multiple draft bills were subsequently introduced before the final enactment of the DPDP Act, 2023.

III. OBJECTIVES AND SCOPE

A. Digital Personal Data Protection Act, 2023

The DPDP Act primarily regulates the processing of digital personal data within India. It applies to data collected in digital form as well as to digitised offline data, and it possesses extraterritorial application where entities outside India process personal data in connection with offering goods or services to individuals in India.[6] The legislation aims to protect the personal data of individuals, recognise the rights of data principals, impose obligations upon data fiduciaries, establish accountability mechanisms for data processing, and facilitate the lawful and transparent use of personal data. The Act excludes certain categories of processing, including personal or domestic use, and grants specific exemptions to the State.

B. General Data Protection Regulation

The GDPR applies to the processing of personal data of individuals residing within the European Union by both public and private entities. It possesses broad territorial reach and applies even to organisations outside the EU if they process data relating to EU residents. The GDPR seeks to protect fundamental rights and freedoms relating to personal data, ensure the free movement of personal data within the EU, harmonise privacy laws across member states, and promote transparency and accountability in data processing. Unlike the DPDP Act, the GDPR provides an extensive and detailed regulatory framework applicable across multiple sectors and processing activities.

[5] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); see also the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

[6] The Digital Personal Data Protection Act, 2023, § 3 (India).

 [ISSN 2581-5369]

IV. KEY PRINCIPLES OF DATA PROCESSING

The GDPR explicitly establishes several core principles governing lawful data processing.[7]

Lawfulness, fairness, and transparency. The principle of lawfulness requires that personal data be processed only where there is a valid legal basis. Fairness ensures that individuals are not misled or treated unjustly during data processing, and transparency requires organisations to provide clear and understandable information about how personal data is collected, used, and stored.

Purpose limitation. Personal data must be collected only for specified, explicit, and legitimate purposes. Organisations are prohibited from using data for unrelated purposes unless a separate legal basis exists. This principle prevents misuse and function creep.

Data minimisation. Organisations should collect only the data necessary to achieve a specific purpose. Excessive or unnecessary collection of personal information is discouraged because it increases privacy risks and the potential for misuse.

Accuracy. Data controllers are required to ensure that personal information remains accurate and up to date. Incorrect information may adversely affect individuals and must therefore be corrected or deleted without undue delay.

Storage limitation. Personal data should not be retained indefinitely. Organisations must establish retention policies and delete information once the purpose for which it was collected has been fulfilled.

Integrity and confidentiality. Appropriate technical and organisational safeguards must be implemented to protect data from unauthorised access, accidental loss, destruction, or alteration. This principle forms the foundation of data-security obligations.

Accountability. The accountability principle requires organisations not only to comply with data protection requirements but also to demonstrate such compliance through documentation, audits, policies, and governance measures.

These principles form the foundation of GDPR compliance and impose strict obligations upon data controllers and processors. The DPDP Act incorporates similar concepts but in a comparatively simplified manner, emphasising lawful processing based on consent and legitimate uses while requiring data fiduciaries to ensure accuracy, security, and accountability; however, the Act does not articulate these principles with the same degree of detail as the GDPR.

[7] General Data Protection Regulation, art. 5 (principles relating to the processing of personal data).

 [ISSN 2581-5369]

A major distinction lies in regulatory philosophy: the GDPR adopts a highly rights-oriented framework emphasising individual autonomy, whereas the DPDP Act attempts to balance privacy protection with administrative flexibility and economic growth.

V. CONSENT AND LAWFUL PROCESSING

Consent constitutes a central component of both instruments. Under the GDPR, consent must satisfy several requirements.

Freely given. Consent must be provided voluntarily, without coercion, pressure, or undue influence, and individuals must have a real choice as to whether to permit the processing of their data. If a person is compelled to provide consent as a condition for receiving a service that does not genuinely require such processing, the consent may not be valid. This requirement prevents organisations from exploiting a superior bargaining position and ensures that consent remains a meaningful expression of choice.

Specific. Consent must relate to a clearly identified purpose. Organisations cannot obtain broad or blanket authorisation permitting them to use personal data for multiple unspecified activities; the purpose must be clearly communicated. For example, consent obtained for sending promotional emails cannot automatically authorise sharing the individual's information with third-party advertisers.

Informed. Individuals must be provided with adequate information before consent is obtained, understanding what information is collected, why, how it will be used, who will have access to it, and how long it will be retained. This promotes transparency and enables informed decisions.

Unambiguous. Consent must be expressed through a clear affirmative action that leaves no doubt as to the individual's intention. Silence, inactivity, or pre-ticked boxes generally do not constitute valid consent. Valid consent includes actively ticking a checkbox, signing a consent form, or selecting an option indicating agreement.

Revocable at any time. An individual who has provided consent must be able to withdraw it at any time, and withdrawal should be as easy as giving consent. Once consent is withdrawn, organisations must generally cease processing unless another lawful basis exists, reinforcing individual control over personal information.

Organisations are required to provide clear notice of the purpose of data collection and processing. Similarly, the DPDP Act requires consent to be free, specific, informed, unconditional, and unambiguous, and data principals may withdraw consent at any stage. However, the DPDP Act introduces the concept of “legitimate uses,” permitting certain

 [ISSN 2581-5369]

processing without explicit consent in specific situations such as State functions, medical emergencies, and employment-related purposes.[8] The GDPR also recognises alternative lawful bases for processing, including contractual necessity, legal obligations, public interest, and legitimate interests,[9] but these grounds are subject to stricter scrutiny and safeguards than the broader exemptions available under the DPDP Act.

VI. RIGHTS OF INDIVIDUALS

A. Rights under the GDPR

The GDPR provides extensive rights to data subjects. The right to access enables individuals to obtain confirmation whether their personal data is being processed and to receive information about the nature and purpose of such processing. The right to rectification allows individuals to request correction of inaccurate or incomplete information. The right to erasure, popularly known as the "right to be forgotten," allows individuals to request deletion of personal data in certain circumstances, such as where the data is no longer necessary or where consent has been withdrawn. The right to data portability permits individuals to obtain their personal data in a structured, machine-readable format and transfer it to another service provider, enhancing consumer choice and competition. The right to object permits individuals to object to specific forms of processing, particularly direct marketing or processing based on legitimate interests. The right to restrict processing permits individuals, in certain situations, to request temporary suspension of processing while disputes about accuracy or legality are resolved. Finally, the GDPR provides safeguards relating to automated decision-making and profiling, entitling individuals to request human intervention and to challenge decisions, based solely on automated processing, that significantly affect them.

B. Rights under the DPDP Act

The DPDP Act grants data principals several rights. The right to access information entitles individuals to receive information concerning the processing of their personal data. The right to correction and erasure allows individuals to seek correction of inaccurate data and deletion of information no longer required for the purpose for which it was collected. The right to grievance redressal permits individuals who believe their rights have been violated to approach the relevant data fiduciary and, where necessary, the Data Protection Board. The Act also introduces a right to nominate another individual who may exercise these rights in the event of the data principal's death or incapacity. While these rights resemble certain GDPR protections, the

[8] The Digital Personal Data Protection Act, 2023, § 7 (India) (legitimate uses).
[9] General Data Protection Regulation, art. 6 (lawfulness of processing).

 [ISSN 2581-5369]

Indian legislation does not explicitly recognise rights such as data portability or objection to automated profiling; consequently, the GDPR offers comparatively broader protection for individual autonomy.

VII. OBLIGATIONS OF DATA FIDUCIARIES AND CONTROLLERS

Under the GDPR, data controllers and processors must adopt extensive compliance measures. They must conduct Data Protection Impact Assessments where processing is likely to pose significant risks to individuals, helping to identify and mitigate privacy risks before processing begins; maintain records of processing activities to facilitate regulatory oversight and demonstrate compliance; appoint Data Protection Officers in specified situations to oversee compliance, provide advice, and liaise with regulatory authorities; report data breaches to the supervisory authority within seventy-two hours, and inform affected individuals where significant risks exist;[10] and implement privacy by design and by default, incorporating data protection considerations into systems and processes from the outset.

The DPDP Act imposes obligations upon data fiduciaries to ensure security safeguards, erase data after the purpose has been fulfilled, and notify breaches to the Data Protection Board and to affected individuals. Significant Data Fiduciaries may also be required to appoint Data Protection Officers and to conduct periodic audits. The GDPR, however, establishes more rigorous and detailed compliance obligations than the comparatively streamlined framework under the DPDP Act.

VIII. CROSS-BORDER DATA TRANSFERS

Cross-border data-transfer regulation represents another significant point of divergence. The GDPR permits the transfer of personal data outside the European Economic Area only where adequate protection measures exist.[11] These include **adequacy decisions** by the European Commission, which may determine that a country provides an adequate level of protection, so that transfers to such countries are permitted without additional safeguards; **standard contractual clauses,** by which organisations use approved contractual provisions to ensure that transferred data receives equivalent protection; **binding corporate rules,** by which multinational corporations adopt internal rules governing transfers within their corporate group; and **explicit consent** of the individual concerned in limited circumstances. The GDPR therefore prioritises maintaining equivalent privacy protection during international transfers.

[10] General Data Protection Regulation, art. 33 (notification of a personal data breach to the supervisory authority).
[11] General Data Protection Regulation, arts. 44-49 (transfers of personal data to third countries or international organisations).

 [ISSN 2581-5369]

The DPDP Act adopts a more flexible approach. It allows the transfer of personal data to countries notified by the Central Government unless specifically restricted.[12] This liberalised framework aims to facilitate global business operations and digital trade while preserving governmental discretion regarding restricted jurisdictions.

IX. Enforcement mechanisms and penalties

The GDPR establishes independent supervisory authorities within each EU member state, possessing broad investigative and corrective powers, including the ability to impose substantial penalties. Administrative fines under the GDPR may reach EUR 20 million or four per cent of the organisation's annual global turnover, whichever is higher.[13] The DPDP Act establishes the Data Protection Board of India to adjudicate disputes and enforce compliance, and monetary penalties under the Act may extend up to Rs. 250 crore for significant violations.[14] Although both instruments impose substantial penalties, the GDPR framework is generally regarded as more stringent owing to its institutional independence, detailed compliance requirements, and strong enforcement mechanisms.

X. Government exemptions and surveillance concerns

One of the most debated aspects of the DPDP Act concerns the broad exemptions granted to the Central Government. The Act permits exemptions for reasons such as sovereignty, public order, and national security.[15] Critics argue that these provisions may weaken privacy protections and enable excessive State surveillance. The GDPR also permits certain exemptions relating to national security and public interest; however, such exemptions remain subject to stronger judicial oversight and proportionality requirements within the European legal framework. This distinction reflects differing constitutional and political approaches to balancing privacy with governmental authority.

XI. Comparative analysis

A comparative evaluation reveals that both the DPDP Act and the GDPR seek to regulate personal data processing and to enhance accountability within the digital ecosystem; however, their regulatory intensity and philosophical orientation differ considerably. The GDPR adopts a comprehensive rights-based model emphasising transparency, accountability, and individual empowerment, imposing extensive obligations upon organisations and establishing robust

[12] The Digital Personal Data Protection Act, 2023, § 16 (India).
[13] General Data Protection Regulation, art. 83(5).
[14] The Digital Personal Data Protection Act, 2023, sch. (India) (penalties).
[15] The Digital Personal Data Protection Act, 2023, § 17 (India) (exemptions).

 [ISSN 2581-5369]

enforcement institutions; consequently, it is considered one of the most advanced data protection frameworks globally.

The DPDP Act, while inspired by international standards, reflects India's socio-economic and governance priorities, seeking to create a balanced framework that protects privacy while enabling digital innovation and administrative efficiency. Critics argue, however, that the Act's broad governmental exemptions, limited individual rights, and comparatively weaker oversight mechanisms may reduce its effectiveness. Despite these concerns, the DPDP Act represents a landmark development in Indian digital governance, establishing foundational privacy protections and introducing accountability standards previously absent from India's legal framework.

XII. Challenges and Future Prospects

The implementation of both instruments presents practical and institutional challenges. For the GDPR, organisations frequently face **complex compliance obligations** that require significant legal, technical, and administrative resources, which can be particularly burdensome for small and medium-sized enterprises; **high implementation costs** relating to compliance audits, technological upgrades, legal consultation, and staff training; **cross-border regulatory coordination** difficulties arising from differences in enforcement priorities among member states; and challenges in the **interpretation of evolving technological practices,** as rapid developments in artificial intelligence, machine learning, and big-data analytics continue to raise new questions about the application of GDPR provisions.

In India, major challenges include limited public awareness of privacy rights, infrastructural and compliance burdens for businesses, the need for institutional capacity-building, and ambiguities regarding governmental exemptions and delegated rule-making. Future reforms may involve strengthening the independence of regulatory authorities, enhancing judicial oversight, clarifying procedural safeguards, and expanding individual rights. As India's digital economy continues to expand rapidly, the effectiveness of the DPDP Act will significantly influence the future of privacy governance in the country.

XIII. Conclusion

The Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation represent significant legal responses to the growing challenges of data privacy in the digital era. While both share the common objective of regulating personal data processing and protecting individuals from the misuse of information, their approaches differ substantially in terms of structure, enforcement, and regulatory philosophy. The GDPR establishes a stringent and

 [ISSN 2581-5369]

comprehensive privacy regime centred upon individual rights and institutional accountability, whereas the DPDP Act adopts a comparatively flexible framework that balances privacy protection with governmental and economic interests. Although the Indian legislation draws inspiration from global standards, it remains less extensive than the GDPR in several important respects, particularly concerning individual rights, regulatory independence, and limitations on State power.

Nevertheless, the enactment of the DPDP Act marks a transformative moment in India's legal and technological landscape, reflecting India's recognition of privacy as a crucial component of democratic governance and digital trust. With effective implementation, institutional strengthening, and future reforms, the Act possesses the potential to evolve into a robust privacy framework capable of addressing emerging technological and societal challenges.

*****

 [ISSN 2581-5369]

XIV. REFERENCES

1. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
2. Regulation 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
3. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).
4. Directive 95/46/EC (Data Protection Directive), 1995 O.J. (L 281) 31.
5. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
6. GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES (Oxford Univ. Press 2014).
7. PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE (Springer 2017).

*****

 [ISSN 2581-5369]